SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

DYNAMIC HARDFILE SIZE ALLOCATION TO SECURE DATA

Field of the Invention

[0001] The present invention relates generally to computer system user data security, and more specifically to access control/protection of nonvolatile memory systems like computer hardfiles.

Background of the Invention

[0002] Although the manufacture and use of a hardfile for a computer system is well known, the industry continues to develop solutions for enhancing the security and availability of the computer systems, and the components used in these computer systems. The development of security systems to restrict and control access to computer system resources and user data and applications has caused an undesirable side effect.

[0003] There are many reasons why an unauthorized user of the computer system resources and user data of a computer system should at times be permitted to have limited access to the operating system of the computer system, and various hardware/software utilities. For example, in the case when a computer technician installs new hardware for use with the computer system, the technician often needs to boot the computer system into an operational mode to properly configure the hardware and the computer system to use the new hardware. Sometimes one or more new software applications must be installed or existing applications may need to be modified. For existing computer systems, an administrator of a secured machine has had two options: 1) permit general access to the computer system, the resources and the user data and applications, or 2) deny the technician access. Sometimes access is enabled by properly entering special security information, for example a login

identification and a password. When an administrator happens to be present and available, the administrator is able to enter the special security information to enable the technician to access the computer system.

[0004] In some cases the technician's access to computer system resources or application data is limited by the operating system according to a limited-permissions account. Unfortunately, many changes to the computer system require access privileges for the technician that are not properly limited by a non-administrator account. Further, the technician sometimes performs the services at times or locations when and where there is no administrator physically present. The administrator is often left with the unpleasant decision to forego the installation or to give security access information to the technician over the telephone or through other means that compromises the security of the computer system.

[0005] Further, administrators are responsible for safeguarding the computer systems and user applications/data not just from authorized access, but also from possible data loss or corruption through inadvertent or malicious users or applications. Also, misinstallation of some hardware and/or software has been attributed as contributing to data loss and corruption. Therefore it may be desirable to have an administrator confirm the technician's installation and run virus or other pest detection programs prior to enabling full operational mode of the installation or otherwise enables access to the entire enterprise.

[0006] Accordingly, what is needed is a system and method for enabling reconfiguration of the computer system to allow for partial access to a hardfile by the operating system, utilities and in some cases certain applications of the computer system while preserving user data and applications. The present invention addresses such a need.

Summary of Invention

[0007] A system and method for access control of a hardfile responsive to a computer system having an operating system is disclosed. The method includes detecting a special boot condition during a pre-boot test of the computer system; and altering, in response to the special boot condition, an operating system access configuration of the hardfile. The system includes a computer system that adjusts an operating system

access to a hardfile based upon various boot conditions.

[0008] The present invention efficiently addresses reconfiguration of a computer system to provide for two or more operational modes, with each mode providing increasingly more (or less) access to computer resources and/or user applications and data. The reconfiguration is most preferably set automatically responsive to a special boot condition detected during a pre-boot procedure of the computer system. Upon detecting the special boot condition, a hardfile is reconfigured to permit the operating system to have access to as much of the hardfile as indicated by the special boot condition. The reconfiguration is performed at the hardware level and the operating system is unable to access any deselected parts of the hardfile.

Brief Description of Drawings

[0009] Figure 1 is a general-purpose computer system for use with a hardfile according to a preferred embodiment;

[0010] Figure 2 is a schematic block diagram of a reconfiguration of a hardfile according to a preferred embodiment; and

[0011] Figure 3 is a flowchart for a preferred embodiment of the invention.

Detailed Description

[0012] The present invention relates to computer system data security and integrity. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment and the generic principles and features described herein will be readily apparent to those skilled in the art. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

[0013] Figure 1 is a general-purpose computer system 100 for use with a hardfile 105 according to a preferred embodiment. The general construction of computer system 100 is well-known, including a central processing unit (CPU) or microprocessor unit (MPU) interconnected by one or more internal buses to computer subsystems (e.g.,

memory, I/O (keyboard, mouse, monitor, for example), communication systems (modem and network, for example), and storage units (volatile and non volatile, and fixed or removable, of many different types). Computer system 100 typically operates under program control, the program most commonly stored on non-volatile computer readable media, such as for example hardfile 105, a hard drive, read-only memory (ROM). The programs, and the set of instructions, are executable by computer system 100 to perform the identified procedures of the code. The particular selection and configuration may vary widely depending upon many different factors.

[0014] The present invention is adaptable to many different kinds of computer systems for many different uses, so the specific details of computer system 100 are not shown but described in very general fashion. A common factor among general-purpose computer systems 100 is that an operating system and user data and application software are installed and accessed from hardfile 105. In most cases, hardfile 105 is physically integrated with computer system 100. In other instances, hardfile 105 may be physically removed or distinct from computer system 100. For example, hardfile 105 may be connected to computer system 100 by a local area network (LAN) or wide-area network (WAN). In some cases, hardfile 105 may include removable media.

[0015] In these various configurations, hardfile 105 includes non-volatile memory for storing an operating system used by computer system 100, and typically user data and application software. Most commonly, hardfile 105 is a fixed harddrive storing the information on magnetic media. Computer system 100 includes a harddrive adapter for controlling the storage and retrieval when hardfile 105 is a harddrive. Computer system 100 will typically include other control and data interfaces when hardfile 105 is not a harddrive, but adapting the present invention to such alternate hardfile systems is within the skill of a person of ordinary skill in the art and would be achieved from this disclosure without undue experimentation. To simplify the discussion, the preferred embodiment will be described in the case that hardfile 105 is a harddrive.

[0016]

In the preferred embodiment, hardfile 105 complies with applicable standards for an ATA/ATAPI-4 (NCITS 314-1998) or later compliant harddrive, the standard hereby expressly incorporated by reference for all purposes. Hardfile 105 must include at

least one partition, and in some cases, there may be multiple logical partitions accessible to computer system 100. In the ATAPI-4 standard, hardfile 105 may be established optionally with an additional partition referred to as a Protected Area Run Time Interface Extension Services or simply PARTIES partition prior to loading the operating system. The PARTIES partition often is set by computer system 100 using a firmware interface (PARTIES) for controlling and accessing this PARTIES partition, and is invisible or otherwise non-accessible to most conventional computer subsystems or conventional routines of the operating system. The PARTIES partition is used to store administration or non-user data. ATAPI-4 provides a procedure called SETMAX that adjusts the size of this PARTIES partition. The preferred embodiment of the present invention uses this SETMAX procedure in a way not contemplated by the standard to provide a novel use of the PARTIES partition to secure data. NCITS can be reached at www.ncits.org.

[0017] In operation and also as well known, various conditions will initiate a power on self-test (POST) of computer system 100. The POST checks various hardware and software conditions of computer system 100 as part of a pre-boot procedure. In the typical scenario, the POST determines that computer system 100 is in condition for operation. Computer system 100 dynamically sets the SETMAX parameter to provide full access to the operating system to complete the boot-up procedure, as well as to provide full access to the user data and application software stored in a different part of hardfile 105.

[0018] In the event that the POST detects a special pre-boot condition, computer system 100 dynamically adjusts SETMAX to exclude all or a portion of hardfile 105 from access by the operating system. The special boot condition may be any type of hardware, software or firmware condition that, in the particular application, would suggest limiting access to part of hardfile 105.

[0019] In the preferred embodiment, a hardware tamper indication detected during the POST causes computer system 100 to dynamically configure SETMAX. The reconfiguration sets the PARTIES partition large enough to exclude the region of hardfile 105 that includes user data and software applications while providing computer system 100 with access to the operating system and any

diagnostic/remedial tools or utilities.

[0020] Adjusting SETMAX in this fashion is advantageous over prior art solutions that either suspended or aborted the boot or ignored the condition and issued a warning. Both solutions are at times unsatisfactory, in contrast to the flexibility of the preferred embodiment.

[0021] When the hardware/software tamper was consequential to a legitimate reconfiguration of computer system 100, the limited hardfile access permits the technician, operator or administrator to test the reconfiguration without exposing the user data and software applications to possible loss or corruption due to bad hardware/software or misinstallation. By using the PARTIES partition in this fashion, computer system 100 is unable to access those portions of hardfile 105 storing the data and software applications, greatly decreasing the risk.

[0022] When the hardware/software tamper was consequential to an unauthorized access of computer system 100, the limited hardfile access isolates the user data and software applications from unauthorized access or destruction, again greatly decreasing any risk to the user data.

[0023] It is an advantage that computer system 100 is operational, and selected portions of the functionality may be configured to be available at all times. Computer system 100 is therefore able to assist in evaluating the post-tamper changes and to aid an administrator in deciding whether to restore computer system 100 to full functionality.

[0024] Adjusting SETMAX to its original value restores computer system 100 to full functionality. Depending upon the desired application, the preferred embodiment either resets SETMAX when the tamper condition is cleared, or after a manual flag is set/cleared by use of a utility application.

[0025] Figure 2 is a schematic block diagram illustrating dynamic reconfiguration of hardfile 105 according to a preferred embodiment. According to the preferred embodiment, hardfile 105 is configured to include at least two distinct (physical or logical) storage areas, but preferably three. A first region 200 of hardfile 105 includes the PARTIES partition, a second region 205 includes the user data and application

software, and a third region 210 includes the operating system. Computer system 100, by use of a hardfile controller 215 for example, sets a SETMAX value 220 as discussed above to include or exclude second region 205 from access by the operating system of computer system 100.

[0026] Hardfile 105 illustrates the full operational mode when SETMAX value 220 allows the operating system access to both first region 200 and second region 205. Hardfile 105' illustrates a limited operational mode when SETMAX value 220' allows the operating system access to only first region 200.

[0027] Figure 3 is a flowchart for a preferred embodiment of the invention implemented by computer system 100. Computer system 100 performs a pre-boot test at step 300 to test for any type of hardware, software or firmware condition that, in the particular application, would suggest limiting access to part of hardfile 105, or, to test whether a previously limited access should be changed or expanded. Computer system 300 tests, at step 305, whether any special boot condition was detected at step 300.

[0028] If the test at step 305 is yes, computer system 100 sets the configuration parameter of hardfile 105 to the appropriate level, given the detected pre-boot condition. For example, if a hardware tamper is detected and hardfile 105 is an IDE/ATAPI-4 harddisk, computer system 105 sets SETMAX to a smaller size than the full readable size of the harddisk and limits the size to a minimum for operating system access. If for example the boot condition is a clearing of a previous tamper condition and hardfile 105 is an IDE/ATAP-4 harddisk, computer system 100 sets SETMAX to be larger and include more of hardfile 105 for access.

[0029] After setting the configuration parameter at step 310, computer system 100 completes the boot sequence at step 315. At step 305, if computer system 100 does not detect a special boot condition, computer system 100 performs step 315 and completes the boot sequence without altering the configuration parameter of hardfile 105.

[0030] While the preferred embodiment has been described in terms of a dual operational mode for hardfile 105, the present invention is not so limited. In some applications, it may be desirable or beneficial to provide for three or more operational modes of

hardfile 105. In this application, various pre-boot conditions may lead to degrees of access to user data or software applications. In some embodiments, user credentials being made available before the SETMAX value is established can provide for increased data security over user/permission based access systems.

[0031] Also, the preferred embodiment uses the SETMAX value to achieve reconfigurable access control to regions of the hardfile. This access control uses physical arrangement and placement of data structures in conjunction with adjustment of the SETMAX value. The present invention contemplates other mechanisms for identifying and segregating the hardfile. Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.